Gouvernance des données

Définition

La gouvernance des données représente l'ensemble des procédures, règles, normes, responsabilités et paramètres qui assurent que les données sont exploitées de façon efficiente, sécurisée et efficace au sein de l'entreprise.

Bonnes pratiques
La culture data
Tirer parti des données pour piloter son entreprise

Gestion des données

Le data management, ou gestion des données est le **processus de collecte, de traitement, de stockage, de partage et d'utilisation des données** au sein d'une organisation et de son écosystème. Ces processus doivent être sécurisés, efficaces et conformes aux réglementations afin d'apporter une valeur ajoutée à l'organisation.

IBM - Data Management

Plan de gestion des données

Étapes :

1. **Identifier les données à collecter** dans le cadre de votre projet, ainsi que la manière dont elles seront collectées et stockées.
2. **Déterminer les normes et les formats** qui seront utilisés pour stocker et documenter, en vous basant sur les normes de l'industrie ou les exigences de l'organisme de financement.
3. **Décrire la méthodologie**, c'est-à-dire la manière dont elles seront gérées tout au long du cycle de vie, en précisant les rôles et les responsabilités de l'équipe chargée de ce projet.
4. **Déterminer les politiques de sécurité et de confidentialité** qui seront mises en place pour protéger les données collectées, y compris les mesures contre les cyberattaques.
5. **Prévoir la conservation et la sauvegarde à long terme**, y compris les politiques de sauvegarde et de récupération.
6. **Décrire la diffusion et le partage** en prenant en compte les politiques de partage des données de votre organisme de financement ou de l'industrie.
7. **Évaluer les coûts engendrés** tout au long du projet, y compris les coûts liés à l'infrastructure de stockage, aux politiques de sécurité, à la formation et aux frais administratifs.

Sauvegardes

Une stratégie de sauvegarde fondée sur les meilleures pratiques n'a pas besoin d'être une boîte

noire. Voici 10 façons d'y parvenir :

- **Élaborer une stratégie**

planifier soigneusement pour s'assurer que toute stratégie de sauvegarde répond aux exigences de l'organisation.
Cette démarche s'inscrit dans le cadre de la planification de la reprise après sinistre et de la continuité des activités.

- **Identifier les données à sauvegarder**

La découverte et la classification des données constituent une première étape essentielle du processus.
Toutes les données ne sont pas forcément jugées suffisamment critiques pour justifier une sauvegarde.
Elles doivent être classées en fonction de l'impact potentiel sur l'entreprise en cas d'indisponibilité.

- **Suivez la règle du 3-2-1**

Trois copies des données, sur deux supports différents, avec une copie stockée hors site et hors ligne.

- **Chiffrez et protégez vos sauvegardes**

Étant donné que les acteurs de la menace recherchent également les copies de sauvegarde des données à des fins d'extorsion, il est utile de les chiffrer afin qu'ils ne puissent pas monnayer les données qui y sont stockées.
Cela ajoutera une couche de défense supplémentaire au mécanisme 3-2-1 (au moins 3 copies, 2 types de stockage différents, 1 copie hors site) si vous l'utilisez.

- **N'oubliez pas les données en nuage (SaaS)**

Une grande partie des données d'entreprise réside désormais dans des applications SaaS (Software-as-a-Service).
Il est utile d'ajouter une couche de protection supplémentaire en sauvegardant ces données également.

- **Testez régulièrement vos sauvegardes**

Vous devez les tester régulièrement pour vous assurer que les données sont sauvegardées correctement et qu'elles peuvent être récupérées comme prévu.

- **Effectuez des sauvegardes à intervalles réguliers**

La régularité des sauvegardes dépend du type d'activité de l'entreprise. Une boutique en ligne très fréquentée nécessitera des sauvegardes presque continues, tandis qu'un petit cabinet d'avocats pourra se contenter d'une fréquence moins élevée.

Réglementation - Aspects juridiques

Règlement général sur la protection des données (RGPD)

Le RGPD est une législation européenne qui encadre le traitement des données personnelles, y compris celles de santé, avec des obligations spécifiques pour les hôpitaux qui souhaitent utiliser des solutions de Big Data :

1. **Consentement éclairé** : Les patients doivent être informés et donner leur consentement pour l'utilisation de leurs données.
2. **Minimisation des données** : Seules les données strictement nécessaires au projet doivent être collectées et utilisées.
3. **Anonymisation et pseudonymisation** : Les données doivent être anonymisées ou pseudonymisées pour limiter les risques de réidentification des patients.
4. **Droits des patients** : Les patients doivent pouvoir exercer leurs droits (accès, rectification, suppression de leurs données).
5. **Notification des violations de données** : En cas de violation de données, l'hôpital doit notifier la CNIL (Commission Nationale de l'Informatique et des Libertés) et, si nécessaire, les patients concernés.

Code de la santé publique

Le Code de la santé publique impose des obligations spécifiques pour les acteurs du secteur de la santé. Les hôpitaux doivent s'assurer que le traitement des données respecte les règles de confidentialité et de sécurité établies par la législation française :

- **Secret médical** : Les professionnels de santé sont soumis à une obligation stricte de secret médical, qui doit être respectée lors du traitement des données.
- **Traitement des données de santé** : Le traitement de données de santé à des fins de recherche, d'analyse ou de gestion hospitalière doit être effectué dans un cadre légal et encadré par des autorisations spécifiques, telles que l'agrément de la CNIL.

Hébergement des données de santé (HDS)

Les hôpitaux qui souhaitent externaliser le stockage ou le traitement des données doivent faire appel à un hébergeur certifié Hébergeur de Données de Santé (HDS), conformément à l’article L1111-8 du Code de la santé publique. Cette certification garantit que l’hébergeur respecte des normes de sécurité strictes, spécifiques aux données de santé.

Intervention de la CNIL

- **DPIA (Data Protection Impact Assessment)** : Les hôpitaux doivent effectuer une Analyse d’Impact relative à la Protection des Données (AIPD) lorsqu’ils mettent en place des projets de Big Data impliquant des données sensibles comme les données de santé. Ce processus vise à évaluer les risques pour la vie privée des patients. CNIL - AIPD
- **Autorisation préalable** : Pour certains traitements de données, notamment ceux impliquant des recherches ou des croisement de grandes quantités de données, une autorisation spécifique de la CNIL peut être nécessaire.

Interconnexion et partage des données

- **Interopérabilité** : Les systèmes de gestion des données doivent être interopérables avec les autres systèmes de santé tout en garantissant un haut niveau de sécurité.
- **Partage sécurisé** : Lorsque des données sont partagées avec d'autres institutions (hôpitaux, chercheurs, etc.), il est crucial de mettre en place des protocoles de sécurité robustes pour garantir la protection des données.

Sécurité des systèmes d’information

La sécurité informatique est un aspect crucial du traitement des données de santé. En France, les hôpitaux doivent respecter les normes de sécurité informatique, notamment le RGS (Référentiel Général de Sécurité) qui fixe les exigences pour garantir la confidentialité, l’intégrité et la disponibilité des systèmes d'information.

Recherche et innovation

Pour l’utilisation des données dans le cadre de la recherche médicale ou d’essais cliniques, des autorisations spécifiques de la part du Comité de Protection des Personnes (CPP) et de la CNIL peuvent être requises. De plus, les projets de recherche doivent suivre les principes éthiques et la protection des droits des patients.

Contrats avec les prestataires externes

Si l'hôpital fait appel à des prestataires externes (fournisseurs de solutions de Big Data, prestataires de services cloud, etc.), il est essentiel que des contrats solides soient établis, incluant des clauses sur la confidentialité, la sécurité des données, la conformité au RGPD et à la législation française.

From:
https://wiki.ox2.fr/ - **Ox2**

Permanent link:
https://wiki.ox2.fr/doku.php?id=cesi:grandoral:benchmark:bigdata

Last update: **2024/09/16 12:16**